Department of Homeland Security Daily Open Source Infrastructure Report for 4 February 2009

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- According to KRQE 13 Albuquerque, investigators said it appears that white powder that was sent to a staff member at an Albuquerque, New Mexico school in an envelope Monday is not a dangerous biological chemical. Ten people were taken to a hospital as a precaution. (See item **15**)
- WTOV 9 Steubenville reports that Bellaire, Ohio residents are permitted to use water again after crews accidentally added about 40 pounds of hydrochloric acid to the water system instead of fluoride on Sunday. A supplier accidentally gave the plant hydrochloric acid instead of fluoride. (See item **21**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *February 2, Reuters* – (National) **More than 470,000 still without power in Midwest.** More than 470,000 homes and businesses were still without power February 1 after snow and ice storms January 27-28 left nearly 1.7 million customers in the dark from Oklahoma to Pennsylvania, local utilities reported. The storms hit Kentucky the hardest, leaving more than 700,000 customers without power. E.ON U.S., which owns Louisville Gas and Electric Co and Kentucky Utilities Co, said it could take seven to ten days to restore service to all 138,000 customers still without service. In Arkansas, another hard hit state, the electric cooperatives, which serve about 490,000 customers, said outages

peaked at about 300,000. The co-ops still had more than 70,000 homes and businesses in the dark Monday morning.
Source: http://news.yahoo.com/s/nm/20090202/us_nm/us_utilities_storm_outages

2. *February 2, Reuters* – (Gulf of Mexico) **Enbridge Nautilus offshore gas line shut due to leak.** Enbridge Inc's U.S. unit said it declared force majeure on February 1 due to a leak on its 30-inch, 101-mile Nautilus natural gas pipeline in the Gulf of Mexico. "Nautilus Pipeline Co, LLC has been shut in at Ship Shoal 207 due to a leak on the pipeline. Under initial investigation damage appears to have been done by an anchor being dragged across the system," a Web site posting said. The company said it was acquiring "personnel, materials, and vessels" for repair, but the pipeline system would remain out of service until further notice.
Source: http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN0245424120090202

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *February 3, Reuters* – (Florida) **Progress sees Fla. Crystal River 3 reactor back soon.** Progress Energy Inc was returning to service the 838-megawatt nuclear Unit 3 at the Crystal River power station in Florida, a spokeswoman for the plant said on February 3. After exiting an outage last week and reaching about 60 percent power, operators noticed a problem with a feed water valve not opening as anticipated. The company fixed the valve and shut the unit on February 2 for post-maintenance testing. The outage last week started on January 27 as workers were calibrating equipment when some blown fuses caused a bus in the switchyard to trip. That resulted in the loss of a feed water booster pump and a condensate pump, which led operators to shut the reactor.
Source: http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN0327208520090203

[Return to top]

Defense Industrial Base Sector

4. *February 3, Washington Post* – (National) **Marines' new ride rolls out years late.** The Marine Corps is starting to deploy a jeeplike vehicle called the Growler, 10 years after conception and at twice the contract price, after delays that were caused by changing concepts and problems in contracting, development and testing, according to two

reports. The idea for such a vehicle was developed in 1999 by the Marine Corps, which wanted a vehicle that could be carried in the V-22 Osprey aircraft to support assault operations and that would tow a 120mm mortar and an ammunition trailer. The first Growlers in the mortar program — officially called internally transportable vehicles, or ITVs — have been deployed to Marine units, but with limited combat capabilities. Because of their light armor and ammunition safety problems, "you can't run it up the highway in an urban area such as Iraq," said the Marines' program manager for the vehicle. "But it could accompany foot-mobile Marine infantry in a not-built-up area such as Afghanistan," he added.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2009/02/02/AR2009020202969.html?hpid=sec-nation

5. *February 2, Army Times* – (National) **Army helos to get diagnostic sensors.** The Army is installing diagnostic devices on thousands more of its helicopters to find problems earlier, leaders said. The service, which has since 2001 equipped 302 Apache attack choppers and 309 Black Hawk utility choppers, plans to equip all 3,300 of its Apaches, Black Hawks, Chinooks, and Kiowa Warriors by 2015. About 500 helicopters a year will get the devices, called digital source collectors, said the director of condition-based maintenance (CBM) in Huntsville, Alabama. The Army is introducing CBM, which depends on small diagnostic devices, as a way to increase the efficiency of maintenance efforts and to spot problems early. Recent Army studies show that the devices have reduced mission aborts by 30 percent, reduced scheduled maintenance by five percent to ten percent, and cut down maintenance test flights by 20 percent. The collectors also have proved useful after mishaps. "We had an event where we lost an aircraft that had some instrumentation on it," the CBM director said. "We recorded the data from the incident and were able to see when the crew lost control of the tail rotor."
Source: http://www.armytimes.com/news/2009/02/defense_army_diagnostics_020209/

6. *February 2, Lockheed Martin* – (National) **First SBIRS satellite with new flight software completes key test at Lockheed Martin.** The first Space-Based Infrared System (SBIRS) geosynchronous orbit (GEO-1) satellite, built by a Lockheed Martin team for the U.S. Air Force, has successfully completed a major test utilizing new flight software. The SBIRS program is designed to provide early warning of missile launches, and simultaneously support other missions including missile defense, technical intelligence, and battlespace awareness. The successful test of the GEO-1 spacecraft, known as Baseline Integrated System Test (BIST), was conducted from January 2, to January 27, 2009 at Lockheed Martin's Space Systems facilities in Sunnyvale, California. The test characterized the performance of the integrated satellite and established a performance baseline prior to entering thermal vacuum testing.
Source: http://www.spaceref.com/news/viewpr.html?pid=27485

[Return to top]

Banking and Finance Sector

7. *February 2, Bloomberg* – (National) **Fed says most U.S. banks tightened terms on loans.** A majority of U.S. banks made it tougher for consumers and businesses to get

credit in the past three months even as lenders received infusions of taxpayer funds, a Federal Reserve report showed today. "About 65 percent of domestic banks reported having tightened lending standards on commercial and industrial loans to large and middle-market firms," the Federal Reserve said in its quarterly Senior Loan Officer survey. "Large fractions of domestic banks continued to report a tightening of policies on both credit-card and other consumer loans." Today's report may underscore concern among Presidential Administration officials and some U.S. lawmakers that banks that have received more than $200 billion of taxpayer funds are failing to lend that on to customers. The Treasury Secretary plans to unveil an overhaul of the government's financial-bailout program next week, an administration aide said. The survey showed that lending overall was only slightly less restrictive than in the third quarter, when the Lehman Brothers Holdings Inc. failure reverberated throughout the financial system. The Fed noted that nearly all banks surveyed tightened standards on commercial real-estate loans last year.
Source:
http://www.bloomberg.com/apps/news?pid=20601103&sid=aB_mZZruz7_o&refer=us

8. *February 2, Idaho Business Review* – (Idaho) **Bank card 'phishing' scams with new twists target Idahoans.** Criminals trying to obtain credit and debit card numbers have expanded their attack on Idaho consumers, the Idaho attorney general warned today. Idaho First Bank in McCall has informed the attorney general's office that numerous people have contacted the bank to report suspicious e-mails, text messages and cell phone calls. Idaho First Bank is not sending these messages. The fraudulent messages are designed to appear that they came from the bank and ask recipients to provide their credit or debit card number. The cell phone calls play a recording that asks the recipient to immediately enter their card account number through the cell phone. Last week, the Idaho attorney general warned consumers not to respond to fraudulent text messages that looked like they came from Bank of the Cascades. There have also been recent news reports of similar messages fraudulently claiming to be from a credit union in Yakima, Washington.
Source: http://www.idahobusiness.net/archive.htm/2009/02/02/Bank-card-phishing-scams-with-new-twists-target-Idahoans

9. *February 2, Pacific Business News* – (Hawaii) **Hawaii bankers warn of phone scam.** Credit and debit cardholders in Hawaii are targets of a new phone "phishing" scam, said the Hawaii Bankers Association. In the scam, an automated recorded message identifying the caller as representing a local bank asks for the person's credit or debit card number and PIN number. "No legitimate financial institution will ever solicit its customers for personal account information over the phone or online," said the association in a statement. Anyone who has responded to questionable phone calls or e-mails are asked to contact their bank's customer-service department.
Source: http://www.bizjournals.com/pacific/stories/2009/02/02/daily8.html

10. *February 2, Nextgov* – (National) **GAO: Bank Secrecy Act data at risk of disclosure.** Ineffective information security controls at an anti-fraud agency within the Treasury Department have left sensitive personal and financial data vulnerable to abuse,

according to a Government Accountability Office report released on January 30. Auditors found that Treasury's Financial Crimes Enforcement Network (FinCEN) allowed multiple users to share accounts to download data, maintained poor control of passwords and accounts, failed to restrict access to sensitive files and did not encrypt all sensitive data. In addition, security guards did not inspect laptop computers entering and exiting the FinCEN facility, increasing the risk that an unauthorized user could introduce malicious software or remove sensitive data without permission, the report (GAO-09-195) stated. "As a result [1970 Bank Secrecy Act] data — containing highly sensitive personal and financial information about private individuals that is used by the law enforcement community to identify and prosecute illegal activity — are at an increased risk of unauthorized use, modification, or disclosure," GAO stated.
Source: http://www.nextgov.com/nextgov/ng_20090202_4418.php

[Return to top]

Transportation Sector

11. *February 2, Global Security Newswire* – (California) **Los Angeles hotel chemical dump sparked terrorism fear.** Employees of a luxury hotel in downtown Los Angeles sparked fears of terrorism two weeks ago when they allegedly dumped nearly 100 gallons of chlorine and muriatic acid down a rooftop drain, the Los Angeles Times reported Saturday. Fumes from a storm drain outside the Standard hotel spread to a nearby subway station early on January 19, causing two or more people to vomit and producing a burning feeling in the eyes and lungs of a Los Angeles County sheriff's deputy. "Chlorine is not naturally occurring…and the subway is a venue we anticipated as a target. So I thought this was actually a terrorist attack," said the head of the FBI's WMD response team in Los Angeles. His team, along with hazardous material crews from the Los Angeles Police and Sheriff's departments, searched the subway station before discovering the source of the gas near the hotel. An adjacent intersection had to be closed off for hours because fumes were still emanating from the storm drain. Maintenance personnel at the hotel, which has a rooftop pool, first acknowledged dumping a limited amount of chlorine down the drain. Under continued pressure from the FBI, they admitted that much more of the chemical had been dumped. The company that owns the hotel was formally accused Thursday of knowingly disposing of hazardous waste, a charge that carries a fine up to $500,000.
Source: http://www.globalsecuritynewswire.org/gsn/nw_20090202_2660.php

12. *February 2, Associated Press* – (National) **Pilots: FAA taking too long on useful bird radar.** The government is taking too long to develop a useful bird-detecting radar that might prevent incidents like last month's dramatic splashdown of a US Airways airliner, officials for the nation's largest pilots union said February 2. It has been 10 years since the National Transportation Safety Board recommended the Federal Aviation Administration (FAA) develop a radar system that enables airline pilots to avoid birds. The FAA is testing experimental systems at some airports, but agency officials caution the technology is unproven and still needs years of refinements. "That is not a satisfactory timeframe," said the Air Line Pilots Association's (ALPA) safety chairman, a Boeing 767 captain. ALPA included the bird problem among the union's top safety

priorities for 2009. Radar has been capable of detecting birds for many years, but to be useful to pilots it must also identify the altitude of the birds and their distance from an airport. Most collisions between birds and airliners take place under 3,000 feet when aircraft are taking off or landing.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5i4uNSCQjTwaVkosn1uX4EvfC7UIQD963NJ9O0

13. *February 2, Fresno Bee* – (California) **Probe cites alcohol in fatal plane crash.** A pilot who crashed his private airplane in Selma early last year had been drinking "within hours" of the flight and probably was impaired, the National Transportation Safety Board (NTSB) has concluded. A man from Sanger, California crashed his Beechcraft Bonanza in a vineyard just minutes after taking off from Fresno's Chandler Downtown Airport on January 18, 2008. The pilot had a blood-alcohol level of 0.07 percent at the time of the crash, "sufficient to result in impairment," according to the NTSB report issued Thursday.
Source: http://www.wkowtv.com/Global/story.asp?S=9769134&nav=menu1362_1

14. *February 2, DarkReading* – (National) **Drive-by 'war cloning' attack hacks electronic passports, driver's licenses.** With a $250 used RFID scanner he purchased on eBay and a low-profile antenna tucked away in his car, a security researcher recently drove the streets along Fisherman's Wharf in San Francisco, where he captured and cloned a half-dozen electronic passports within an hour. The researcher, who is the technical lead for research and testing in information security at eBay, coined this newest RFID attack "war cloning." The security weaknesses of the EPC Gen 2 RFID tags have been well-known for some time. These tags are being used in the new wallet-sized passport cards that the U.S. Department of Homeland Security offers under the new Western Hemisphere Travel Initiative for travel to and from Western Hemisphere countries. Unlike previous RFID hacks that have been conducted within inches of the targeted ID, his hack can scan RFID tags from 20 feet away. "This is a vicinity versus proximity read," he says. "The passport card is a real radio broadcast, so there's no real limit to the read range. It's conceivable that these things can be tracked from 100 meters — a couple of miles." He says the RFID chip technology found in traditional passport books is better because it has encryption and authentication features. He suggests the Federal Government replace the e-passport RFID chips with the RFID chips used in the passport books.
Source:
http://www.darkreading.com/security/privacy/showArticle.jhtml;jsessionid=35LA4DR1HIG4KQSNDLRSKHSCJUNN2JVN?articleID=213000321

[Return to top]

Postal and Shipping Sector

15. *February 2, KRQE 13 Albuquerque* – (New Mexico) **Investigators: White powder not deadly.** Investigators in Albuquerque, New Mexico said it appears that the white powder, which was sent to a staff member at Taft Middle School in an envelope

Monday, is not a dangerous biological chemical. Presumptive tests show the powder is not life threatening, but it has been sent to a state lab for additional testing. “It’s an oxiding type of powder, maybe something you find in a cleaner that’s why we’re getting signs of respiratory distress from the folks inside you breath it in, it’s an irritant, but again we take this serious,” a New Mexico National Guard official said. In all, 10 people were taken to University of New Mexico Hospital as a precaution. The administrator, who opened the envelope, said she immediately had trouble breathing. She was taken to a quarantined area and sent to the hospital. Four other teachers and support staff, who were around at the time, were also taken to the hospital. One resource officer and four Los Ranchos fire fighters, who arrived at the scene first, were also sent to the hospital. State Police said the envelope did not have a return address or letter inside it. It was addressed to Taft Middle School, in care of a staff member. “It was mailed and the postal service has responded, and their inspectors are going to be looking into who sent the letter,” the APS police chief said. The students were put on lockdown and all left safely just after 3:00 p.m.
Source:
http://www.krqe.com/dpp/news/crime/crime_krqe_albuquerque_taft_powder_20090202 1550

[Return to top]

Agriculture and Food Sector

16. *February 3, Yankton Press and Dakotan* – (National) **Group files suit over farm pollution exemption.** A lawsuit was filed recently against the U.S. Environmental Protection Agency (EPA) by a coalition of groups challenging a last minute rule of the former Presidential Administration that exempts factory farms from reporting toxic emissions to government officials. The environmental law firm Earthjustice filed the suit on behalf of the groups, arguing that the exemption will harm people living and working near factory farms. The new rule was issued December 12, 2008 by the EPA in conjunction with a ruling that also exempts an estimated 118,500 tons of hazardous waste annually from strict federal incineration controls. According to the Environmental Integrity Project, an increasing body of scientific evidence shows that ammonia, hydrogen sulfide and other factory farm emissions can pose threats to human health and the environment.
Source:
http://www.yankton.net/articles/2009/02/03/community/doc4987d848737c9431096602.t xt

17. *February 3, Associated Press* – (Texas) **Firm tied to salmonella ran unlicensed Texas plant.** A peanut processing plant in Texas run by the same company blamed for a national salmonella outbreak operated for years uninspected and unlicensed by government health officials, the Associated Press has learned. The Peanut Corp. of America plant in Plainview never was inspected until after the company fell under investigation by the U.S. Food and Drug Administration, according to Texas health records obtained by AP. Once inspectors learned about the Texas plant, they found no sign of salmonella there. But new details about that plant — including how it could have

operated unlicensed for nearly four years — raise questions about the adequacy of government efforts to keep the nation's food supply safe. Texas is among states where the FDA relies on state inspectors to oversee food safety. In Texas, the inspector of the Department of State Health Services was sent to Plainview, in the sparsely populated Texas Panhandle, after salmonella was traced to the company's plant in Georgia. The inspector said the Texas plant was not licensed with health officials and had never been inspected since it opened in March 2005. Texas requires food manufacturers to be licensed every two years and routinely inspected. The plant is registered with the Texas Comptroller of Public Accounts to do business as Plainview Peanut Co. LLC, according to state records. But the company "was unable to present evidence at the time of the inspection of a current food manufacturers license," the inspector wrote in his report.
Source: http://www.google.com/hostednews/ap/article/ALeqM5jeLgwCG-FEEYH8KZ7Tt45zOdSIKgD963VQ800

18. *February 2, InjuryBoard.com* – (National) **Proposed FDA Globalization Act will help prevent Salmonella outbreaks, preserve food safety, and ensure consumer rights.** Recently, Congressman from Michigan introduced a plan to update the Food and Drug Administration (FDA) which, according to the American Association for Justice, "would help ensure the safety of the nation's food, drugs, medical devices and cosmetics and help restore confidence in the safety of the nation's products. The FDA's Globalization Act, if approved, would impose registration fees on processing plants to help fund food safety initiatives, would increase the frequency of manufacturing facility inspections to once every four years, would raise the penalties for noncompliance with FDA regulations, and would ensure more widespread safety-testing of imported food products. It would also give the FDA greater authority to recall products it deems potentially harmful to consumers.
Source: http://cherryhill.injuryboard.com/fda-and-prescription-drugs/proposed-fda-globalization-act-will-help-prevent-salmonella-outbreaks-preserve-food-safety-and-ensure-consumer-rights.aspx?googleid=256524

19. *February 2, RFID News* – (Hawaii) **Hawaiian agencies launch food safety pilot program.** The State of Hawaii Department of Agriculture and the Hawaii Farm Bureau have partnered for a three-year pilot RFID program designed to promote food safety by enabling product visibility throughout the supply chain. The Hawaii Produce Traceability initiative uses RFID technology to track fresh produce down to the farm, or even field, level. Growers can participate by either slap-and-ship tagging or usage of a hand-held RFID system. State officials are now planning for the next two phases of the initiative. Enhancements may include RFID-enabled cellphones to enable more farms to participate, and implementing produce temperature tracking to reduce the threat of food spoilage. The program may eventually be expanded to cover 5,000 Hawaiian farms.
Source: http://www.rfidnews.org/2009/02/02/hawaiian-agencies-launch-food-safety-pilot-program

[Return to top]

Water Sector

20. *February 3, Arkansas Democrat Gazette* – (Arkansas) **Water suppliers need generators, state official says.** An Arkansas Department of Health engineer said he is interested in requiring water providers to have backup power to make sure water keeps flowing when the electricity goes out. The Health Department's engineering section director made the comments about the need for backup power on February 2 as more than 60 drinking water systems across north Arkansas remained under a precautionary boil order because of the ice storm. "We have a Health Department requirement in our regulations that they have an emergency plan, but it's not specific about what's contained in that plan," he said. "At least for me, this ice storm has demonstrated that we need to be more specific in that plan about how to ensure that they will have water if they lose power or lose a primary source of water." Bigger drinking water systems in north Arkansas have largely avoided the boil orders because they have backup power supplies, he said. The Arkansas Rural Water Association has three diesel-powered generators, which cost $110,000 in all, available to members. Generators provided by rural water associations in Louisiana and Mississippi were loaned to water systems in Arkansas during last week's storm, said the director of the association in Arkansas.
Source: http://www.nwanews.com/adg/News/251337/

21. *February 3, WTOV 9 Steubenville* – (Ohio) **Bellaire chemical mix-up in water 'very serious mistake.'** Bellaire, Ohio residents are permitted to use water again after crews accidentally added hydrochloric acid to the system instead of fluoride. A supplier, Ohio Valley Chemical, accidentally gave the plant hydrochloric acid instead of fluoride, said the superintendent of the water department. He said workers at the treatment inadvertently added about 40 pounds of hydrochloric acid to the system on Sunday. They realized the mistake Monday morning when they saw fluoride levels were lower than normal. "It was a mistake. It could happen to anybody. It was a very serious mistake, (but) it could have been worse," he said. He said the fact that the wrong acid was delivered — and ended up in the water system — was both the department's and the suppliers' fault. He said Ohio Valley Chemical, based in Martins Ferry, is not the department's usual supplier. To remedy the problem, crews opened up hydrants and drained the system, tanks, and water plant. Police said the water was deemed safe as of 12:30 p.m. Tuesday. Because officials did not immediately know how much acid was in the water, customers were initially urged to avoid using tap water, and classes at Bellaire High School were dismissed at 8:15 a.m. The incident affected between 2,300 and 2,400 people, officials said.
Source: http://www.wtov9.com/news/18621661/detail.html

[Return to top]

Public Health and Healthcare Sector

22. *February 3, Wausau Daily Herald* – (National) **Marshfield Clinic involved in study to test medical data-sharing.** Researchers at Marshfield Clinic want to speed up their understanding of rare diseases and find cures by learning how to store, share and use medical records created by universities and clinics across the country. The clinic, the University of Wisconsin-Madison and the University of Michigan are taking part in a pilot project led by Case Western Reserve University in Cleveland to test the

effectiveness of a system. The group will share records on sleep disorders because diagnosing sleep apnea involves large amounts of data, said the doctor, who leads the Marshfield Clinic Research Foundation's efforts to better apply information technology to health and medical research. The Federal Government awarded the coalition up to $4 million for more than two years to create and test such a system. Marshfield Clinic will receive about $112,000.
Source:
http://www.wausaudailyherald.com/article/20090203/WDH0101/902030546/1981

23. *February 2, Johns Hopkins University* – (National) **HIV transmission rate declines in United States, study finds** Although the number of people living with HIV has increased in the United States over time, the rate at which an infected person passes the virus on to an uninfected person has dropped significantly since the peak of the epidemic, according to a study by researchers at the Johns Hopkins Bloomberg School of Public Health and the Centers for Disease Control and Prevention. Researchers found the rate of transmission has dropped 88 percent since 1984 and 33 percent since 1997. The study will be published in JAIDS: Journal of Acquired Immune Deficiency Syndromes and is available on the journal's Web site in advance of publication.
Source: http://www.eatg.org/eatg/Global-HIV-News/Epidemiology/HIV-transmission-rate-declines-in-United-States-study-finds

[Return to top]

Government Facilities Sector

24. *February 3, Associated Press* – (Nebraska) **White powder found in Nebraska state building safe.** Authorities have determined there were no toxic substances on an envelope containing a white, powdery substance found at the State Office Building in Lincoln. The envelope was found on the morning of February 2 on the sixth floor. Workers in the area were removed, but the building was not evacuated. The deputy Lincoln fire chief said the substance was not immediately identified, but no one appeared to have been sickened by it.
Source:
http://www.siouxcityjournal.com/articles/2009/02/03/news/latest_news/doc4988485d67bc2081861791.txt

[Return to top]

Emergency Services Sector

25. *February 2, WTMJ 4 Milwaukee* – (Wisconsin) **OpenSky still offline.** More than five years after signing on the dotted line, "OpenSky," a multi-million dollar, state-of-the-art communications system for Milwaukee's first responders still doesn't work. Now, high-level elected leaders feel it may be time to cancel the project. The $15 million system would have allowed Milwaukee police, fire, EMS, all first responders, talk to each other in real time. While the system in its current state allows police officers can hook up laptop computers and hard-wired radios in their squad cars to the system, the handheld

radios first responders rely on failed in a recent round of live tests. “It became clear that we were having problems with dead spots and some operator problems that were certainly distressing our police officers and creating an environment where they felt unsafe,” explained Milwaukee’s police chief. City records show the project’s deadline has been pushed back over and over again to November 2005, then for another two months, then to June 2006, again to August 2007, and now even further into 2009.
Source: http://www.msnbc.msn.com/id/28972027/

26. *February 2, Associated Press* – (Maryland) **Company claims Md. EMS delaying mass casualty study.** A Bel-Air, Maryland, company is accusing the state’s emergency medical service of delaying the release of a study of a new method for triaging patients in mass casualty incidents. The company, ThinkSharp, believes its method could save lives and that the Maryland Institute for Emergency Medical Services System, the independent agency that oversees emergency medicine statewide, has been sitting on the study too long. The institute’s executive director said the delay stemmed from discussions about what a paper should say. He said the method needs to be studied further and some paramedics found the method confusing and difficult to use.
Source: http://www.baltimoresun.com/news/health/bal-ems-report0202,0,4482888.story

[Return to top]

Information Technology

27. *February 2, DarkReading* – (International) **Glitch causes Google to issue false malware warnings.** A glitch in Google over the weekend rendered the site virtually inoperative for almost an hour and falsely warned users that the sites they were searching contained malware. According to a statement by the vice president of search products and user experience at Google, the problem was “very simply, human error. Google flags search results with the message ‘This site may harm your computer’ if the site is known to install malicious software in the background or otherwise surreptitiously. They do this to protect our users against visiting sites that could harm their computers. “We periodically receive updates to that list and received one such update to release on the site [Saturday] morning,” the vice president continued. “Unfortunately, the URL of ‘/’ was mistakenly checked in as a value to the file and ‘/’ expands to all URLs. Fortunately, our on-call site reliability team found the problem quickly and reverted the file,” the vice president said. “Since we push these updates in a staggered and rolling fashion, the errors began appearing between 6:27 a.m. and 6:40 a.m. and began disappearing between 7:10 and 7:25 a.m., so the duration of the problem for any particular user was approximately 40 minutes.” Google initially blamed StopBadware, an industry group that collects and updates a list of malware sites, for the problem. However, the source of the problem actually resided in Google’s own malware list, according to news accounts. Google says the problem is now fixed, so if users get a message that a particular site may contain malware, they should heed it.
Source:
http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml;jsessionid=35LA4DR1HIG4KQSNDLRSKHSCJUNN2JVN?articleID=213000451

28. *February 2, Computerworld* – (International) **Study: Data breaches continue to get more costly for businesses.** Companies that are reluctant to invest what it takes on data security better be prepared to pay a lot more if their systems are ever breached. That's the main take-away from a new report released by the Ponemon Institute LLC, which shows that the average cost of a data breach to companies is continuing to increase. Ponemon said the breaches from last year that it studied cost an average of about $202 for each compromised customer record. That is 46 percent higher than the $138 per record that Ponemon cited in its first annual report on breach costs, for 2005. The average cost had previously increased to $182 in 2006 and $197 in 2007, according to Ponemon. The cost-per-record figures include direct expenses for breach detection, mitigation, notification and response efforts, as well as indirect costs, such as the financial impact of customer defections and lost business opportunities. Ponemon said the average overall cost of the breaches covered in the new report was more than $6.6 million, with individual companies reporting costs that ranged from $613,000 to almost $32 million. The report was based on a study of breaches at 43 large companies from 17 different industries. The number of customer records that were compromised in the breaches ranged from less than 4,200 to more than 113,000.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9127147&taxonomyId=17&intsrc=kc_top

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

29. *February 3, Telx* – (New Jersey; New York) **Telx chooses AboveNet dark fiber to link New York Metro area data centers.** Telx, an interconnection and colocation data center operator, has chosen AboveNet, a fiber optic connectivity provider, to link its New York and New Jersey-based data centers with dark fiber. Customers installing equipment in one of Telx's four New York area facilities will have low latency in their connections between these locations, and the option to connect directly to more than 500 other carrier and enterprise customers over a Telx-managed optical transport network. The new AboveNet dark fiber optical network connects Telx's four primary New York metro area data centers by using diverse fiber routes with two separate Hudson River crossings. "Physical path diversity was a critical design element of the network to ensure the highest reliability for customers, especially those working in top-tier financial services where there is zero tolerance for network interruption. In addition, the dark fiber and optical transport offers the lowest possible latency for customers connecting to financial institutions' networks that are colocated in Telx facilities, such as Gargoyle

Strategic Investments LLC. and ACTIV Financial," said the executive vice president of engineering and operations at Telx.
Source: http://biz.yahoo.com/bw/090203/20090203005204.html?.v=1

30. *February 2, CNET News* – (International) **Sony points to finger veins for gadget security.** Sony is taking biometrics from the surface of the finger to the inside with a new vein authentication technology that could show up on mobile devices within the year. The compact, camera-based system, called "Mofiria," uses a CMOS sensor to diagonally capture scattered light inside the finger veins. Data from the pattern is compressed, making it possible for the information to be stored on gadgets like laptops or cell phones. Sony says vein authentication technology achieves higher accuracy and produces faster reads than other biometric authentication techniques, such as fingerprint or retinal scans. Finger vein patterns differ from person to person and finger to finger, Sony noted, and do not change over the years. Also, they're much easier to remember than passwords. Sony claims that false rejection rate for the system is less than 0.1 percent and processing time for identification takes only about 0.015 seconds using a personal computer CPU and about 0.25 seconds using a mobile-phone CPU.
Source: http://news.cnet.com/8301-17938_105-10154711-1.html?part=rss&tag=feed&subj=News-Security

31. *February 2, Salt Lake Tribune* – (National) **Extender boosts cell phone signals.** Verizon Wireless has started selling a book-sized device that boosts cell phone signals within a home for $250, making it easier for people to drop a home phone line and rely solely on wireless. The Verizon Wireless Network Extender needs to be connected to a broadband Internet line. Then it acts a miniature cellular tower, listening for signals from a subscriber's cell phone. It covers up to 5,000 square feet. Such devices are known as "femtocells." Verizon Wireless, the country's largest carrier, is following in the footsteps of Sprint Nextel Corp., which started selling a femtocell under the Airave brand nationwide last year. The Airave costs $100, but Sprint charges an extra $5 per month for use. Verizon Wireless is not charging a monthly fee.
Source: http://www.sltrib.com/technology/ci_11610177

32. *February 2, San Antonio Express-News* – (Arkansas; Oklahoma; Texas) **AT&T data outage lasts four hours.** Dallas-based wireless telecommunications giant AT&T Inc. has repaired a wireless network outage that left some customers in San Antonio and other parts of Texas, Oklahoma and Arkansas unable to use data services for more than four hours on February 2. The outage made it impossible for many customers to send and receive data via the company's high-speed 3G network and over its older wireless data network, EDGE. Affected devices displayed a message saying, "data connection refused." The outage was the result of a cut in a large-capacity fiber-optic line, an AT&T spokesman said. The company restored service around 3 p.m.
Source: http://www.mysanantonio.com/business/38834267.html

[Return to top]

Commercial Facilities Sector

33. *February 2, Associated Press* – (California) **Rockfall in Yosemite lands near popular hotel.** Yosemite National Park managers say a rockfall last week launched small flying granite fragments into the parking lot behind the historic Ahwahnee Hotel. Most of the 800 tons of rock that fell on January 29 landed on a slope behind the historic hotel in Yosemite Valley. There were no injuries, but officials said February 1 a car windshield was damaged.
Source: http://www.lasvegasnow.com/global/story.asp?s=9775958

[Return to top]

National Monuments & Icons Sector

34. *February 3, Denver Post* – (Colorado) **Carcasses dumped at monument.** A pile of more than 700 pounds of elk and cattle body parts was discovered last month in the Canyons of the Ancients National Monument in southwestern Colorado, according to federal authorities. Investigators with the U.S. Bureau of Land Management (BLM) are now looking for whoever used the monument land as a dump site. Bones had been sawed, and the pieces are likely a byproduct, or waste, from animals that were processed for food, said a BLM law enforcement ranger. He discovered the dump site in mid-January on a routine patrol when he followed tire tracks to the edge of a ravine. Vandals have also struck in the area, known as Goodman Point, destroying signs and trailhead facilities. The illegal dump and vandalism happened roughly within the same time frame and are physically near each other. Perpetrators could face up to a $100,000 fine and a one-year prison sentence if convicted. The monument contains more than 6,000 American Indian archaeological sites, including ancestral Puebloan sites, on 165,000 acres in the Four Corners region.
Source: http://www.denverpost.com/news/ci_11613777

[Return to top]

Dams Sector

35. *February 1, Thibodaux Daily Comet* – (Louisiana) **Pipelines prove costly obstacles to levee building.** The arteries that pump oil through the remote wetlands of Terrebonne Parish will likely become an expensive hindrance as locals try to move forward with major hurricane-protection and coastal-restoration projects, officials say. The hundreds of pipelines that cross Terrebonne have already begun to complicate the parish's efforts to move forward with levee projects. A six-mile $30 million levee being constructed in Dulac by the U.S. Army Corps of Engineers will be built with four gaps where pipelines cut through it. Corps officials say it is impossible for workers to relocate the pipelines and build a complete levee given time and money constraints. "It's not an obstacle, but it's definitely a cost," said the Terrebonne Levee Board President. "We have to cross 50-something pipelines on Morganza's alignment at a cost of $1 million or more." That's $1 million or more for each pipeline that needs to be moved. Pipelines that run through levees can cause vulnerabilities in tested levees, said a state senator. In Montegut, officials had repeated problems with levees failing at pipeline crossings.
Source: http://www.dailycomet.com/article/20090201/ARTICLES/901319929/-

1/SPORTS?Title=Pipelines_prove_costly_obstacles_to_levee_building

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.
To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer